

# Quantum lost property: A possible operational meaning for the Hilbert-Schmidt product

Matthew F. Pusey\* and Terry Rudolph  
*Department of Physics, Imperial College London,  
 Prince Consort Road, London SW7 2AZ, United Kingdom*  
 (Dated: October 15, 2012)

Minimum error state discrimination between two mixed states  $\rho$  and  $\sigma$  can be aided by the receipt of “classical side information” specifying which states from some convex decompositions of  $\rho$  and  $\sigma$  apply in each run. We quantify this phenomena by the average trace distance, and give lower and upper bounds on this quantity as functions of  $\rho$  and  $\sigma$ . The lower bound is simply the trace distance between  $\rho$  and  $\sigma$ , trivially seen to be tight. The upper bound is  $\sqrt{1 - \text{tr}(\rho\sigma)}$ , and we conjecture that this is also tight. We reformulate this conjecture in terms of the existence of a pair of “unbiased decompositions”, which may be of independent interest, and prove it for a few special cases. Finally, we point towards a link with a notion of non-classicality known as preparation contextuality.

Suppose a system has been prepared in one of two non-orthogonal quantum states. The task of measuring the system in order to estimate which state was used is known as state discrimination [1, 2], an important concept in quantum information theory. The impossibility of succeeding at this task with certainty enables quantum cryptography [3]. Here we investigate a version of state discrimination where, in each run, additional classical information about each of the possible preparations is provided to the agent attempting the discrimination.

*Classical analogy.* Charlie spots the dim outline of a pencil case under his desk. He knows Alice and Bob have both recently lost theirs, and judges the case equally likely to belong to either of them. All the pencil cases at his school are either pink or blue. Charlie believes that girls buy pink pencil cases with probability  $1/2$  whilst boys buy them with probability  $1/4$ . He therefore resolves to return the pencil case to Alice if it is pink, and Bob if it is blue. He calculates the probability of returning the case to its true owner as  $(1 + \delta_C)/2$ , where

$$\delta_C(\{p_i\}, \{q_i\}) = \frac{1}{2} \sum_i |p_i - q_i| \quad (1)$$

is here equal to  $1/4$ . Unsatisfied, he devises a better plan: he will ask Alice and Bob what colour their pencil cases actually are, returning it to whoever states the correct colour. The only way this strategy can fail is if Alice and Bob happen to have bought the same colour, in which case Charlie is forced to toss a coin. Hence his probability of success is slightly better,  $(1 + P_{\text{diff}})/2$  where

$$P_{\text{diff}}(\{p_i\}, \{q_i\}) = 1 - \sum_i p_i q_i \quad (2)$$

is  $1/2$  in this case.

*Definitions.* Fix a finite dimensional Hilbert space  $\mathcal{H}$ . The optimum probability of discriminating two states

$\rho, \sigma \in L(\mathcal{H})$  (with equal priors) is  $(1 + \delta)/2$ , where the quantum trace distance  $\delta$  is given by [4]

$$\delta(\rho, \sigma) = \frac{1}{2} \text{tr} |\rho - \sigma|. \quad (3)$$

Decomposing  $\rho = \sum_i p_i \rho_i$  and  $\sigma = \sum_j q_j \sigma_j$  ( $p_i, q_j > 0$ ,  $\rho_i, \sigma_j$  states), we can define the average trace distance

$$\Delta(\{p_i\}, \{\rho_i\}, \{q_j\}, \{\sigma_j\}) = \sum_{i,j} p_i q_j \delta(\rho_i, \sigma_j). \quad (4)$$

If, when attempting to distinguish two states  $\rho$  and  $\sigma$ , we are told in each run which (independently sampled)  $\rho_i$  and  $\sigma_j$  applies, the best strategy is clearly to optimally distinguish  $\rho_i$  from  $\sigma_j$ . The overall probability of success will then be  $(1 + \Delta)/2$ .  $\Delta$  was briefly mentioned in Ref. [5], but a different quantity  $D^K$  where the product distribution  $p_i q_j$  is replaced by an adversely correlated distribution was deemed preferable in that setting.

*Lower bound.* By the joint convexity [4] of  $\delta$ , we have

$$\Delta(\{p_i\}, \{\rho_i\}, \{q_j\}, \{\sigma_j\}) \geq \delta(\rho, \sigma). \quad (5)$$

This bound is saturated by the trivial decomposition  $p_1 = q_1 = 1$ ,  $\rho_1 = \rho$ ,  $\sigma_1 = \sigma$ .

*Upper bound.* By Eq. (5) a decomposition that maximizes  $\Delta$  can always be taken to consist of pure states  $\rho_i = |\psi_i\rangle\langle\psi_i|$  and  $\sigma_j = |\phi_j\rangle\langle\phi_j|$ , and so we consider only this case from now on. Hence [4]  $\delta(\rho_i, \rho_j) = \sqrt{1 - |\langle\psi_i|\phi_j\rangle|^2} = \sqrt{1 - \text{tr}(\rho_i\sigma_j)}$ . Noting that  $\sqrt{1-x}$  is concave [6] on its domain  $x \leq 1$ , the trace is linear, and  $\sum_{i,j} p_i q_j \rho_i \sigma_j = \rho\sigma$ , we have

$$\Delta = \sum_{i,j} p_i q_j \sqrt{1 - \text{tr}(\rho_i\sigma_j)} \leq \sqrt{1 - \text{tr}(\rho\sigma)}. \quad (6)$$

*Saturating the upper bound.* Since  $\sqrt{1-x}$  is in fact strictly concave, equality in Eq. (6) can only be achieved if the arguments  $x$  in each term of sum (except those with zero probability, which we can remove from the decompositions) are equal. Hence the upper bound is tight for

\* m@physics.org

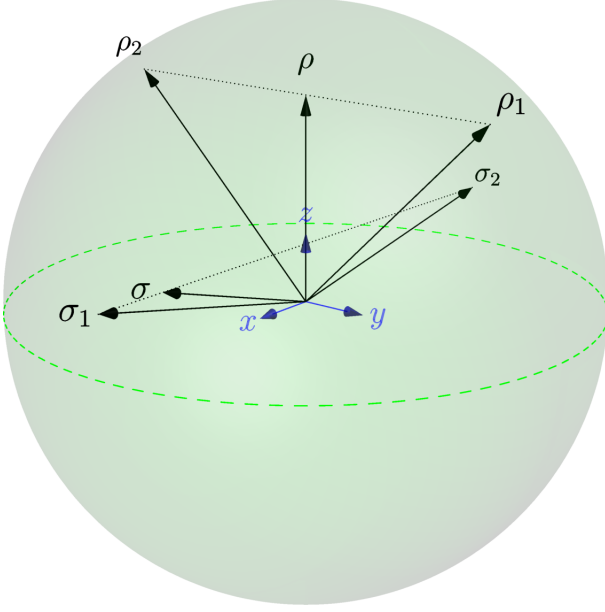


FIG. 1. A pair of unbiased decompositions.

a particular  $\rho$  and  $\sigma$  if and only if there exists decompositions  $\rho = \sum_i p_i |\psi_i\rangle \langle \psi_i|$  and  $\sigma = \sum_j q_j |\phi_j\rangle \langle \phi_j|$  which are “unbiased” in that  $|\langle \psi_i | \phi_j \rangle|^2 = \text{tr} \rho \sigma$ . (Note that by the linearity of the trace, *any* decompositions satisfy the weaker condition  $\sum_{i,j} p_i q_j |\langle \psi_i | \phi_j \rangle|^2 = \text{tr}(\rho \sigma)$ .)

Since numerics indicate that Eq. (6) is tight, we conjecture that a pair of unbiased decompositions exists for any pair of states  $\rho$  and  $\sigma$ . We also make the stronger conjecture that such a pair exists with both decompositions minimal, i.e.  $i \in \{1, \dots, \text{rank}(\rho)\}, j \in \{1, \dots, \text{rank}(\sigma)\}$ . We will now prove some special cases of this conjecture.

*Qubits.* Suppose  $\dim \mathcal{H} = 2$ . Choose a basis so that the Bloch vectors for  $\rho$  and  $\sigma$  are  $\vec{\rho} = (0, 0, r)$  and  $\vec{\sigma} = (s_x, 0, s_z)$  respectively. Then  $\vec{\rho}$  is clearly on the line between the two pure states at  $\vec{\rho}_{1,2} = (0, \pm\sqrt{1-r^2}, r)$ , giving rise to a valid decomposition, and similarly for  $\vec{\sigma}_{1,2} = (\pm\sqrt{1-s_z^2}, 0, s_z)$ . Finally  $\vec{\rho}_i \cdot \vec{\sigma}_j = r s_z = \vec{\rho} \cdot \vec{\sigma}$  and so  $\text{tr}(\rho_i \sigma_j) = \text{tr}(\rho \sigma)$  as required. These decompositions are illustrated in Fig. 1.

*Maximally mixed  $\sigma$ .* Suppose  $\dim \mathcal{H} = d$ , and  $\sigma = I/d$ . Choose a basis  $\{|\psi_i\rangle\}$  in which  $\rho$  is diagonal. Clearly there exists a decomposition using these states. Let  $\{|\phi_j\rangle\}$  form a basis that is mutually unbiased with respect to the  $\{|\psi_i\rangle\}$  basis, for example by using the quantum Fourier transform unitary [4]. We have that  $\sigma = \sum_j q_j |\phi_j\rangle \langle \phi_j|$  with  $q_j = 1/d$  and the decompositions are, by construction, unbiased.

*A useful lemma.* Let  $f$  be a convex-linear map from the set of states on  $\mathcal{H}$  to the real numbers. Then any state  $\rho$  has a decomposition into  $\text{rank}(\rho)$  pure states  $\rho_i$  which all satisfy  $f(\rho_i) = f(\rho)$ .

The proof is as follows. For an arbitrary minimal de-

composition  $\{\rho_i\}$ , consider the figure of merit

$$F = \sum_i |f(\rho_i) - f(\rho)| \quad (7)$$

If  $F > 0$  we can construct a new decomposition with smaller  $F$  as follows. Take  $k$  so that  $f(\rho_k)$  is maximal and  $l$  so that  $f(\rho_l)$  is minimal. Notice that we can “continuously swap”  $\rho_k$  and  $\rho_l$ . More formally, there exists continuous functions  $\rho_k(\theta), \rho_l(\theta)$  with  $\rho_k(0) = \rho_l(\pi) = \rho_k$  and  $\rho_k(\pi) = \rho_l(0) = \rho_l$  such that  $\rho$  can be decomposed into  $\rho_k(\theta), \rho_l(\theta)$  and the  $\rho_i$  with  $i \neq k, l$  for any  $\theta \in [0, \pi]$ . To see this, consider the continuous family of unitaries  $U(\theta)$  with  $U(\theta)|k\rangle = \cos(\theta/2)|k\rangle - \sin(\theta/2)|l\rangle$  and  $U(\theta)|l\rangle = \sin(\theta/2)|k\rangle + \cos(\theta/2)|l\rangle$  and all other  $|i\rangle$  unaffected, and apply Schrödinger’s mixture theorem [7, 8]. Now by the intermediate value theorem there exists a  $\theta^* \in (0, \pi)$  with  $f(\rho_k(\theta^*)) = f(\rho_l(\theta^*))$ . Since by convex-linearity the average value of  $f$  of this new decomposition must still equal  $f(\rho)$ , this procedure must have reduced  $F$ . Finally, since the unitary group is compact, the set of decompositions of  $\rho$  into pure states is compact and hence  $F = 0$  must be achieved for some decomposition.

*Corollary: unbiased decomposition of  $\rho$ .* If  $\rho_i$  and  $\sigma_j$  are unbiased decompositions, then by linearity

$$\text{tr}(\rho_i \sigma) = \sum_j q_j \text{tr}(\rho_i \sigma_j) = \sum_j q_j \text{tr}(\rho \sigma) = \text{tr}(\rho \sigma). \quad (8)$$

Conversely, setting  $f(\cdot) = \text{tr}(\cdot \sigma)$  in the above lemma implies that there always exists a minimal decomposition of  $\rho$  satisfying  $\text{tr}(\rho_i \sigma) = \text{tr}(\rho \sigma)$ . Notice that the proof of the lemma suggests a numerical method for finding such decompositions using a series of one-dimensional search problems, which may sometimes be faster than solving the direct  $(d^2 - 1)$ -dimensional search problem.

*Pure  $\sigma$ .* Suppose that  $\text{rank}(\sigma) = 1$ . By the above corollary we can decompose  $\rho$  into pure states  $\rho_i$  such that  $\text{tr}(\rho_i \sigma) = \text{tr}(\rho \sigma)$ . Since  $\sigma$  is already pure we can take  $\sigma_1 = \sigma$  and we have a pair of unbiased decompositions.

*Rank two  $\sigma$ .* Suppose  $\text{rank}(\sigma) = 2$ . If  $\text{rank}(\rho) = 1$  then we are in the previous case, so assume  $\text{rank}(\rho) \geq 2$ . By the above corollary we can decompose  $\sigma$  into two states  $\sigma_j = |\phi_j\rangle \langle \phi_j|$  satisfying  $\text{tr}(\rho \sigma_j) = \text{tr}(\rho \sigma)$ . Apply the corollary again to obtain a decomposition  $\rho'_i = |\psi'_i\rangle \langle \psi'_i|$  of  $\rho$  satisfying  $|\langle \psi'_i | \phi_1 \rangle|^2 = \text{tr}(\rho'_i \sigma_1) = \text{tr}(\rho \sigma_1) = \text{tr}(\rho \sigma)$ .

Choose a basis  $|1\rangle, \dots, |n\rangle$  ( $n = \text{rank}(\rho) \geq 2$ ) for the support of  $\rho$  such that  $|2\rangle, \dots, |n\rangle$  are orthogonal to  $|\phi_1\rangle$ . Then  $|\psi'_i\rangle$  must be of the form  $\sum_k c_k |k\rangle$  where  $|c_1| = \sqrt{\text{tr}(\rho \sigma) / \langle 1 | \phi_1 \rangle}$ . Furthermore any state  $|\psi\rangle$  of this form also satisfies  $|\langle \psi | \phi_1 \rangle| = \text{tr}(\rho \sigma)$  and such states form a connected set. Since  $\sum_i p_i \text{tr}(\rho'_i \sigma_2) = \text{tr}(\rho \sigma_2) = \text{tr}(\rho \sigma)$  there must be a  $k$  with  $\text{tr}(\rho'_k \sigma_2) \geq \text{tr}(\rho \sigma)$  and an  $l$  with  $\text{tr}(\rho'_l \sigma_2) \leq \text{tr}(\rho \sigma)$ . By the above observations and the intermediate value theorem, there is a state  $|\psi_1\rangle$  in the support of  $\rho$  with  $|\langle \psi_1 | \phi_2 \rangle|^2 = \text{tr}(\rho \sigma)$ .

Let  $p_1$  be maximal, i.e.  $p_1 = 1 / \langle \psi_1 | \rho^{-1} | \psi_1 \rangle$  [4].  $\rho' = (\rho - p_1 |\psi_1\rangle \langle \psi_1|) / (1 - p_1)$  then has  $\text{rank}(\rho') = n - 1$

and also satisfies  $\text{tr}(\rho'\sigma_j) = \text{tr}(\rho\sigma)$ . If  $\rho'$  is pure then take it as  $\rho_2$  and we are done, otherwise iterate the above procedure to obtain  $|\psi_2\rangle$ , and so on.

Numerics (using [9]) indicate that, when  $\text{rank}(\sigma) > 2$ , if one simply takes any decomposition  $\sigma_j$  with  $\text{tr}(\rho\sigma_j) = \text{tr}(\rho\sigma)$  then it is not always possible to find a decomposition of  $\rho$  which is unbiased with respect to that  $\sigma_j$ . This would prevent the above being extended to general  $\sigma$ .

*Preparation contextuality.* Consider the special case  $\rho = \sigma = I/d$ . We have shown that one can find two minimal decompositions of  $\rho$  with  $\Delta = \sqrt{1 - \text{tr}(\rho^2)} = \sqrt{1 - 1/d}$ . If, as suggested by the fact they give rise to the same mixed state, there is no actual difference between these two decompositions, it is somewhat surprising that this is larger than the value we obtain if we instead use two identical minimal decompositions of  $\rho$ , easily seen to be  $\Delta = 1 - 1/d$ .

This can be made precise by supposing that the two decompositions were represented by a preparation non-contextual ontological model [10]. Briefly, this associates each state  $\rho$  with a probability distribution  $\mu_\rho(\lambda)$  over ‘‘ontic states’’  $\lambda$  (representing the physical state of affairs). Preparation noncontextuality is the assumption that this distribution depends only on  $\rho$ . Each ontic state  $\lambda$  and measurement procedure  $M$  gives rise to a probability distribution  $p(k|M, \lambda)$  over outcomes  $k$ , and the quantum statistics are recovered as  $p(k|M, \rho) = \int p(k|M, \lambda)\mu_\rho(\lambda)d\lambda$ . It is not difficult to see that if some measurement procedure  $M$  distinguishes  $\rho$  and  $\sigma$  with probability  $(1+\delta)/2$  then  $\mu_\rho$  and  $\mu_\sigma$  must be distinguishable with probability at least  $(1+\delta_C)/2$ , and so every for every  $\rho$  and  $\sigma$ ,  $\delta_C(\mu_\rho, \mu_\sigma) \geq \delta(\rho, \sigma)$ .

If  $\sum_i p_i \rho_i$  and  $\sum_j q_j \sigma_j$  are minimal decompositions of  $I/d$  then we must have  $p_i = q_j = 1/d$  and in the model

$$\mu_{I/d} = \frac{1}{d} \sum_i \mu_{\rho_i} = \frac{1}{d} \sum_j \mu_{\sigma_j}. \quad (9)$$

Since, as argued above,  $\delta \leq \delta_C$ , we must have

$$\Delta \leq \Delta_C = \frac{1}{d^2} \sum_{i,j} \delta_C(\mu_{\rho_i}, \mu_{\sigma_j}). \quad (10)$$

By considering the regions where  $\mu_0 < \mu_1$  and  $\mu_0 \geq \mu_1$

separately and using normalization it can be shown that  $\delta_C(\mu_0, \mu_1) = 1 - \int \min(\mu_0(\lambda), \mu_1(\lambda)) d\lambda$ . Hence

$$\Delta \leq 1 - \frac{1}{d^2} \int \sum_{i,j} \min(\mu_{\rho_i}(\lambda), \mu_{\sigma_j}(\lambda)) d\lambda. \quad (11)$$

Notice that for any  $j$  and  $\lambda$ ,  $\sum_i \min(\mu_{\rho_i}(\lambda), \mu_{\sigma_j}(\lambda))$  either contains at least one  $\mu_{\sigma_j}$ , or is equal to  $\sum_i \mu_{\rho_i}$  which is equal to  $\sum_k \mu_{\sigma_k}$  by Eq. (9). Either way, it is greater than or equal to  $\mu_{\sigma_j}$  and so

$$\Delta \leq 1 - \frac{1}{d^2} \int \sum_j \mu_{\sigma_j} d\lambda = 1 - \frac{1}{d}, \quad (12)$$

where the equality is by the normalization of the  $\mu_{\sigma_j}$ . This is indeed exactly the value we get by using two identical decompositions  $\rho_i = \sigma_i$ , and so any protocol that has a higher probability of success (for example our optimal one) is a proof of preparation contextuality.

*Conclusions.* The fact that mixed states have many decompositions into pure states is a key feature of quantum mechanics, sometimes considered the definition of non-classicality [11]. We have discussed a task that puts this feature centre stage. Our upper bound on the probability of success provides a fairly direct operational meaning for the Hilbert-Schmidt inner product  $\text{tr}(\rho\sigma)$ .

The main open problem is to prove our conjecture that every pair of states has a pair of unbiased decompositions. A notable special case of that conjecture would be when the states commute. In the other direction, a lower bound on  $\Delta$  when restricted to decompositions into pure states would be more interesting than the trivial lower bound we give for the general case. Finally, it is likely that the connection with preparation contextuality can be extended beyond the very special case we consider.

## ACKNOWLEDGMENTS

We thank K. Audenaert, J. Barrett, F. G. S. L. Brandão, S. Castiglione, G. McConnell and A. Scott for discussions. Both authors are supported by the EPSRC.

- 
- [1] A. Chefles, *Contemp. Phys.*, **41**, 401 (2000), arXiv:quant-ph/0010114.
  - [2] S. M. Barnett and S. Croke, *Adv. Opt. Photon.*, **1**, 238 (2009), arXiv:0810.1970.
  - [3] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, *Rev. Mod. Phys.*, **74**, 145 (2002), arXiv:quant-ph/0101098.
  - [4] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, 2000).
  - [5] O. Oreshkov and J. Calsamiglia, *Phys. Rev. A*, **79**, 032336 (2009), arXiv:0812.3832.
  - [6] S. Boyd and L. Vandenberghe, *Convex Optimization* (Cambridge University Press, Cambridge, 2004).
  - [7] E. Schrödinger, *Proc. Camb. Phil. Soc.*, **32**, 446 (1936).
  - [8] L. P. Hughston, R. Jozsa, and W. K. Wootters, *Phys. Lett. A*, **183**, 14 (1993).
  - [9] C. Spengler, M. Huber, and B. C. Hiesmayr, *J. Math. Phys.*, **53**, 013501 (2012), arXiv:1103.3408.
  - [10] R. W. Spekkens, *Phys. Rev. A*, **71**, 052108 (2005), arXiv:quant-ph/0406166.
  - [11] J. Barrett, *Phys. Rev. A*, **75**, 032304 (2007), arXiv:quant-ph/0508211.